



Learn to protect yourself from viruses, scams and fraud

## TYPES OF FRAUD INVESTIGATIONS

- Bank Fraud (Debit Card Fraud, Check Fraud, Etc.)
- Financial Fraud (Embezzlement, Elder Exploitation, Etc.)
- Identity Theft
- Scams

## TYPES OF SCAMS



- Government/Law Enforcement Scams
- Consumer Scams
- Family/Friend Scams
- Investment Scams
- Romance Scams
- Tech Support Scams

# GOVERNMENT/LAW ENFORCEMENT SCAMS

In these type of scams, the scammer will pretend to be some form of law enforcement (IRS, FBI, or even a local agency). Typically, they will use the fear of potential arrest to persuade you into giving them what they want. Many times, they will ask you to buy gift cards as a form of payment to avoid the arrest. Government Departments/Law Enforcement will never ask for payment to avoid arrest or legal consequences.



# U.S. Customs and Border Protection

doesn't call and ask for money.

But scammers do.

Learn more about these types of scams

– and how to avoid them – at **ftc.gov/imposters**.



### GOVERNMENT / LAW ENFORCEMENT SCAM

if you receive a call from someone reporting to be from a government or law enforcement agency and are asked to provide personal information such as bank account, social security, account login information, etc. OR to purchase gift cards to avoid legal action or to satisfy a warrant -

IT IS A SCAM

Never provide banking or personal account information to anyone.

Gift cards are not used to make payments.



Buying a gift card to pay someone? Stop!

It's a scam.

Gift cards are for gifts, not payments.



Report gift card scams at:

For more information, visit:

ReportFraud.ftc.gov

Ftc.gov/giftcards

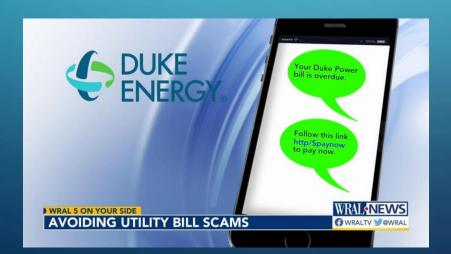


Please warn your friends and family.

Any request to purchase gift cards to pay for something is a scam!

## CONSUMER SCAMS

These scams occur when the scammers pretends to be a well-known company typically one you are a user of. The scammer will then threaten some form of loss or cancelation of service unless they receive payment and/or your financial information.





#### From: no-reply@amazon.com <crw... >

To:

Today at 11:33 AM

#### amazon

Greetings from Amazon,

We have locked your Amazon account and all pending orders.

We have taken this action because the billing information you provided does not match the information on file with the card issuer.

To resolve this issue, please verify now with the billing name, address, and phone number stored on your credit card. if you have recently moved, you may need to update this information with the card issuer.

Check Now

If we cannot complete the verification process within 3 days, all pending orders will be canceled. You will not be able to access your account until this process is complete.

We ask that you do not open new accounts as any new order you place may be delayed.

We appreciate your patience with our security measures. Thank you for your attention.

Best regards, Amazon Service Team

amazon

© 2021 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon. Amazon.com, the Amazon.com logo and 1-Click are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210.

Reference: 874507091

# FAMILY/FRIEND SCAMS

This scam take places when the scammer pretends to be a family member of friend of yours. Usually there is some form of emergency or reason that they need money or your information. Scammers use this scam especially to pry unto your emotions. No one wants to see their child, grandchild, or friend in need and most people are willing to do whatever it takes to help.

#### What can you do?

- To avoid falling prey, ask the caller to prove who they are. Ask them their name. Most scammers know the name of the relative they are posing as.
- Write down the callers phone number.
- They'll ask you not to, but call the child's parents.
- **HANG UP!**







# INVESTMENT SCAMS





Investment Scams happen anytime the scammer offers some sort of opportunity to make money from a small payment or investment. These scams usually result in the scammer needing more and more money from you in order to deliver your "earnings". The best advice for these types of scams is the old saying: "If it sounds too good to be true, it probably is."

## ROMANCE SCAMS

A romance scam occurs when the scammer pretends to be someone (military member, famous actor, etc.) and makes contact with you via phone, text message, or some form of social media. The scammer will engage you in general conversation before quickly professing their love for you. Not long after this, the scammer will request money in some form. Typically, the reason for needing the money is to come and be with you.

#### Signs of a Scam



Professes love quickly.

Claims to be from the U.S., but is overseas for business or military service.



Asks for money, and lures you off the dating site.



Claims to need money

— for emergencies,
hospital bills, or travel.

Plans to visit, but can't because of an emergency.

### Is Your Cyber Sweetheart Swindling You?

Roses are red, violets are blue, and romance scammers can fool you, too. Look for these red flags.



They say they're far away.



Their profile seem too good to be true.



The relationship is moving fast.



They break promises to see you.



They ask for money.



They require specific payment methods.

## Romance scammers use fake identities and back stories to gain your trust.



Don't get scammed. Learn more fcc.gov/consumers

#### TECH SUPPORT FRAUD

Scammers impersonate tech companies and then email or call saying you need to pay to fix a phony tech issue or sign up for a subscription for a fake security service. They also might impersonate a customer service rep for a utility company, a government agency or a bank and tell you there's a problem with your account and they need personal info to fix it.

These scammers will try any means possible: email, phone, text, social media, snail mail, you name it.

But remember, no government agency, including the IRS, will ask for personal information over the phone. And in general, one of the best ways your older loved ones can protect themselves is to never give their personal information to anyone unless they know exactly who the person is and why they need it.

- Ignore unsolicited calls from strangers who tell you there is something wrong with your device. – Know that legitimate tech companies will not contact you to ask for remote access to your computer.
- Make sure all anti-virus / malware software is up to date.
- If you need help, used a company you trust. Ask friends for suggested company if you don't know anyone.

## PREVENTING THESE SCAMS

- Many of these scams are phishing scams which means they are sending them to
  multiple people seeing who will "bite." If you are not expecting the call, email, letter,
  etc., then do not answer or respond.
- Trust your instincts, if you think something sounds suspicious, it probably is.
- If you are ever in doubt, hang up the phone or stop what you are doing, and contact the actual company/department to verify what the scammer is saying. You can also contact someone you trust or even law enforcement to verify your suspicion.
- Gift Cards are gifts and are never used as a form of payment.
- Please understand, these are only the main types of scams we see, there are many more out there. You should always be suspicious when someone asks for money over the phone or internet.

### WARNING SIGNS OF TELEPHONE AND ONLINE SCAMS



Individuals
threatening
you with
arrest or
calling law
enforcement



Individuals
asking for
money,
especially via
a particular
method (i.e.
prepaid debit)



Individuals
calling from
out-of-state
or unknown/
sketchy
company names



# RANDOLPH COUNTY SHERIFF'S OFFICE

#### THREE THINGS TO REMEMBER

1

Law Enforcement and the US Government will NEVER ask for any payment of any form to avoid arrest. 2

Never share personal or financial the don't information over the phone with someone up. I you do not know.

3

If you cannot verify the caller's identity, don't answer or hang up. If you feel unsafe or suspect criminal activity, call 9-1-1.

# TALK TO THE SENIORS IN YOUR LIFE ABOUT TELEPHONE SCAMS

CYBER SECURITY

- Talking about elder fraud and scams with your loved ones is so important. Is it fun? No, usually not. Is it a way to show them how much you care? Yes, 100%.
- One of the most important steps you can take to protect your parents or grandparents from different kinds of elder fraud is to set them up with identity theft protection.
- Register them with the National Do Not Call Registry

#### HELP SENIORS AVOID SCAMS



- CHECK IN OFTEN TO SEE HOW YOUR LOVED ONE IS DOING.
- 2. EDUCATE YOUR LOVED ONE ABOUT THEIR RISK FOR FRAUD -- BOTH FROM SOLICITORS AND FROM PEOPLE THEY KNOW.
- 3. MAKE SURE ANTIVIRUS SOFTWARE IS INSTALLED AND UP-TO-DATE ON THEIR COMPUTER.
- 4. SIGN YOUR LOVED ONE UP FOR A CREDIT MONITORING SERVICE.
- 5. CHECK THEIR PHONE CALL LOGS TO SEE IF THEY'RE BEING INUNDATED WITH TELEMARKETING CALLS.
- 6. REGISTER HIM OR HER WITH THE NATIONAL DO NOT CALL REGISTRY TO CUT THEIR CHANCES OF BEING TARGETED BY PHONE SCAMMERS.
- 7. MEET ANY HOME CARE AIDES HIRED TO HELP YOUR LOVED ONE. MAKE RANDOM VISITS.



#### WHAT DO YOU DO IF YOU'VE BEEN SCAMMED?

- If you or a loved one has been a victim of fraud, contact your bank immediately to report any suspicious transactions. It's also a good idea to call the National Elder Fraud Hotline (1-833-FRAUD-11) to report the crime.
- Getting scammed can make your loved one feel embarrassed, sad and anxious. Don't let them beat themselves up for getting tricked. Walk with them through their emotions, and try your best to help them see the light at the end of the tunnel.

# PROBLEM WITH ANY OF THESE?

•Report it!

ReportFraud.ftc.gov



